



IPSec ポリシーの管理

- [IPsec ポリシーの概要 \(1 ページ\)](#)
- [IPsec ポリシーの設定 \(1 ページ\)](#)
- [IPsec ポリシーの管理 \(2 ページ\)](#)

IPsec ポリシーの概要

IPsec は、暗号セキュリティサービスを使用した IP ネットワーク経由の非公開でセキュアな通信を保証するフレームワークです。IPsec ポリシーが IPsec セキュリティ サービスの設定に使用されます。このポリシーは、ネットワーク上のほとんどのトラフィックタイプにさまざまなレベルの保護を提供します。コンピュータ、部門 (OU)、ドメイン、サイト、またはグローバル企業のセキュリティ要件を満たすように IPsec ポリシーを設定できます。

IPsec ポリシーの設定



- (注)
- システムのアップグレード中、IPsec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPsec ポリシーを作成したり変更したりしないでください。
 - IPsec には双方向プロビジョニングが必要です (ホストまたはゲートウェイごとに 1 ピア)。
 - 一方の IPsec ポリシー プロトコルが「ANY」、もう一方の IPsec ポリシー プロトコルが「UDP」または「TCP」に設定されている 2 つの Unified Communications Manager ノードに IPsec ポリシーをプロビジョニングする場合、「ANY」プロトコルを使用するノードでの検証で検出漏れが発生する可能性があります。
 - IPsec はシステムのパフォーマンスに影響します (特に暗号化した場合)。
-

手順

-
- ステップ1 Cisco Unified OS の管理から [セキュリティ (Security)] > [IPSec の設定 (IPSec Configuration)] の順に選択します。
 - ステップ2 [新規追加 (Add New)] をクリックします。
 - ステップ3 [IPSEC ポリシーの設定 (IPSEC Policy Configuration)] ウィンドウで各フィールドを設定します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。
 - ステップ4 [保存 (Save)] をクリックします。
 - ステップ5 (任意) IPsec を検証するには、[サービス (Services)] > [Ping] の順に選択し、[IPsec の検証 (Validate IPsec)] チェックボックスをオンにして、[Ping] をクリックします。
-

IPsec ポリシーの管理

システムのアップグレード中、IPSec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPsec ポリシーを変更または作成しないでください。



- 注意** ホスト名、ドメイン、または IP アドレスを変更するために既存の IPsec 証明書に変更を加える際、証明書名を変更する場合は、IPsec ポリシーを削除して作り直す必要があります。証明書名を変更しない場合は、リモートノードの作り直した証明書をインポートした後に、IPsec ポリシーを無効にして有効にする必要があります。
-

手順

-
- ステップ1 Cisco Unified OS の管理から [セキュリティ (Security)] > [IPSec の設定 (IPSec Configuration)] の順に選択します。
 - ステップ2 ポリシーを表示、有効、または無効にするには、次の手順を実行します。
 - a) ポリシー名をクリックします。
 - b) ポリシーを有効または無効にするには、[ポリシーの有効化 (Enable Policy)] チェックボックスをオンまたはオフにします。
 - c) [保存] をクリックします。
 - ステップ3 1 つまたは複数のポリシーを削除するには、次の手順を実行します。
 - a) 削除するポリシーの横にあるチェックボックスをオンにします。

[すべてを選択 (Select All)] をクリックするとすべてのポリシーを選択でき、[すべてをクリア (Clear All)] を選択するとすべてのチェックボックスをクリアできます。

- b) [選択項目の削除 (Delete Selected)] をクリックします。
-

